

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: LENOVO ADWARE LITIGATION,

Case No. 15-md-02624-RMW

This Document Relates to All Cases

**ORDER GRANTING IN PART MOTION
TO DISMISS AND MOTION FOR
CLASS CERTIFICATION**

Re: Dkt. Nos. 98, 131

Plaintiffs bring this putative consumer class action against defendants Lenovo (United States), Inc. and Superfish, Inc. asserting claims under federal, California, and New York law. Plaintiffs allege that Superfish's VisualDiscovery software, which Lenovo installed on the laptops they purchased, created performance, privacy, and security issues. Lenovo moves to dismiss plaintiffs' claims for lack of standing and failure to state a claim. Dkt. No. 98. Plaintiffs move to certify three classes of purchasers: a nationwide class of direct purchasers, a nationwide class of indirect purchasers, and a California class of consumers who purchased laptops from third-party retailers. Dkt. No. 131.

Lenovo's motion to dismiss is granted with leave to amend as to plaintiffs' New York General Business Law claim, Electronic Communications Privacy Act claim, Consumer Protection Against Computer Spyware Act claim, California negligence claim, New York

negligence claim, and plaintiffs’ claim for injunctive relief. Lenovo’s motion to dismiss is denied as to all other claims. Plaintiffs’ motion for certification of the indirect purchaser class and the California class is granted. Plaintiffs’ motion for certification of the direct purchaser class is denied.

I. BACKGROUND

Lenovo Inc. is a Delaware corporation with its principal place of business in Morrisville, North Carolina. Dkt. No. 96, Compl. ¶ 18. Lenovo manufactures laptop computers, which it sells directly to consumers and indirectly through stores and online retailers. *Id.* ¶¶ 1, 121-24. Superfish Inc. is a Delaware corporation with its principal place of business in Palo Alto, California. *Id.* ¶ 19. Superfish develops adware programs—in particular, image-to-image search technology that enables consumers to search for items based on the appearance of the item, rather than on the text description. *Id.* ¶¶ 1, 34. Named plaintiffs are six consumers in different states who purchased Lenovo computers with Superfish’s VisualDiscovery software preinstalled. *Id.* ¶¶ 10-17. Plaintiffs assert twelve causes of actions against Lenovo based on the following allegations.

Plaintiffs allege that Lenovo routinely accepts payments from software development companies like Superfish, which has a history of disseminating spyware and malware, to preload software onto Lenovo computers. *Id.* ¶¶ 37-38, 25-27. In early 2014, Superfish and Lenovo began discussing a partnership for the purpose of loading VisualDiscovery onto certain Lenovo computers. *Id.* ¶ 65. VisualDiscovery functions by “intercepting data sent between a computer user and a website, redirecting it for analysis to generate relevant advertisements, and then transmitting those advertisements back to the user’s computer” where the advertisements are injected into the user’s web browser as part of a webpage or in a pop-up ad. *Id.* ¶¶ 2, 40, 42. For example, if a user views the webpage for a stand mixer on a shopping website, VisualDiscovery presents the user with ads featuring similar stand mixer images found on other shopping websites. *Id.* ¶ 42.

VisualDiscovery employs a proxy component that handles web transmissions to and from a user’s web browser, both encrypted and unencrypted. *Id.* ¶¶ 44, 45. When users seek encrypted HTTPS connections, the proxy acts as a “man-in-the-middle” proxy. *Id.* VisualDiscovery

terminates the direct connection between a user's computer and a secure website's server that otherwise would have been established by an HTTPS request and redirects the user's encrypted data to the VisualDiscovery proxy. *Id.* ¶ 46. The proxy decrypts the user's data and transmits certain data to Superfish servers to be analyzed for use in generating advertisements. *Id.* ¶¶ 42, 46. The proxy then re-encrypts the user's data before forwarding it to the originally requested website's server. *Id.* ¶ 46.

In order to decrypt the data sent by users' browsers, VisualDiscovery uses a tool called the "SSL hijacker," that was provided to Superfish by another software company, B.W. Komodia. *Id.* ¶¶ 55-57. The "SSL hijacker" allows VisualDiscovery to impersonate any SSL-enabled site, essentially "vouch[ing] for itself as a trusted root-certificate authority," and presenting Superfish's digital certificate as trusted. *Id.* ¶ 57. During the relevant time period, the private key for this tool—which enables decryption and the creation of an apparently trusted digital certificate—was protected only by a very weak password. *Id.* ¶¶ 50, 61.

While some Lenovo executives expressed concern about VisualDiscovery, Lenovo and Superfish finalized a profit sharing agreement in June 2014. *Id.* ¶¶ 2, 71, 72. Lenovo began shipping laptops with VisualDiscovery installed in August 2014. *Id.* ¶¶ 80-81, 84. Lenovo did not disclose to consumers that VisualDiscovery was installed on its computers, although other third-party software installed on the computers was listed on Lenovo's website. *Id.* ¶ 3. Plaintiffs allege that Lenovo and Superfish buried the software deep within the operating system "to avoid detection by anti-malware programs." *Id.* ¶¶ 3, 85-86. Users were presented with an option to "opt out" the first time they used a web browser on their new laptops, but opting out only disabled VisualDiscovery—it did not remove the software from the laptop. *Id.* ¶ 70.

Plaintiffs allege that VisualDiscovery had a negative impact on the Lenovo laptops. The program "increased CPU usage, which increased power consumption" and decreased both "the lifespan of the battery (number of times it could be recharged before being replaced) and the number of hours that the laptop could operate on a single charge." *Id.* ¶¶ 5, 59. These problems "were so severe that they violated the product specifications of certain Lenovo computer models." *Id.* ¶ 79. VisualDiscovery caused problems with internet connectivity and "subjected users to

1 unwanted advertising and pop-ups that were difficult to remove and to stop.” *Id.* ¶ 5. Plaintiffs also
 2 allege that VisualDiscovery made the Lenovo laptops vulnerable to third-party hackers and other
 3 malicious actors who could take advantage of Visual Discovery’s ability to act as a certificate
 4 authority to conceal their own interception of Plaintiffs’ and other Class members
 5 communications. *Id.* ¶ 60.

6 Lenovo began receiving consumer complaints about VisualDiscovery “almost
 7 immediately.” *Id.* ¶ 90; *see also id.* ¶¶ 95, 97, 100-101, 113. In mid-September 2014, an IT
 8 manager at a major bank “complained that VisualDiscovery was interfering with encrypted sites
 9 and that it was intercepting secure communications by inserting a fake root certificate that
 10 effectively created a MitM attack.” *Id.* ¶ 90. In response to the complaints, “Lenovo claims . . .
 11 that it instructed Superfish to disable the HTTPS functionality of VisualDiscovery at the server
 12 level and that Superfish did so.” *Id.* ¶ 92. “According to Lenovo, Superfish then designed a new
 13 version of VisualDiscovery that would not operate on HTTPS sites and did not contain a self-
 14 signed root certificate.” *Id.* ¶ 93. “This version started to be loaded onto Lenovo computers in
 15 November 2014.” *Id.* Then, “[d]ue to ongoing consumer complaints,” Lenovo “ordered Superfish
 16 to turn off the server connections in January and stopped installing the program on new computers
 17 at the same time.” *Id.* ¶ 110.

18 On February 19, 2015, a computer researcher figured out the password for Superfish’s
 19 certificate authority—“komodia”—and made it public, which increased the security vulnerability
 20 for computers with the original version of VisualDiscovery installed. *Id.* ¶¶ 62-64. Anyone with
 21 the password could extract the Superfish digital certificate and private key and then issue his or
 22 her own digital certificate, which in turn would allow access to whatever information a user
 23 happened to be transmitting. *Id.* ¶¶ 62-64. Lenovo then severed its relationship with Superfish
 24 entirely and provided an automated removal tool and free 6-month subscription to a security
 25 service to consumers. *Id.* ¶ 117. Plaintiffs allege however, that some consumers may not have been
 26 aware of these offers and that the removal tool leaves behind several VisualDiscovery files. *Id.* ¶¶
 118-20.

27 Plaintiffs assert twelve causes of action against Lenovo on behalf of the various classes:

(1) violation of Computer Fraud and Abuse Act; (2) violation of the Electronic Communications Privacy Act;¹ (3) violation of the California's Unfair Competition Law; (4) violation of California's Consumer Legal Remedies Act; (5) violation of California's Computer Crime Law; (6) violation of California's Consumer Protection Against Computer Spyware Act; (7) violation of California's Invasion of Privacy Act; (8) negligence under California law; (9) trespass to chattels under California law; (10) violation of New York's Deceptive Acts & Practice; (11) negligence under New York law; and (12) trespass to chattels under New York law.

II. MOTION TO DISMISS FOR LACK OF ARTICLE III STANDING

"[T]he 'irreducible constitutional minimum' of standing consists of three elements." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *as revised* (May 24, 2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). "Plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* (citing *Lujan*, 504 U.S. at 560-561; *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-181 (2000)). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560). "The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Id.* (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)).

"[N]amed plaintiffs must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong." *Id.* at 1547 n.6 (quoting *Simon v. E. Kentucky Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976)) (internal quotation marks omitted). "'Standing is not dispensed in gross.'" *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734, (2008) (quoting *Lewis v. Casey*, 518 U.S. 343, 358, n. 6 (1996)). "Rather, 'a plaintiff must demonstrate standing for each claim he seeks to press' and 'for each

¹ Count II, for violation of 18 U.S.C. 2512, is asserted against Superfish and Lenovo. Count III, for violation of 18 U.S.C. 2510, is asserted against Superfish only.

form of relief” that is sought.” *Id.* (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006)).

A. Economic Injury

In this case, all twelve of plaintiffs’ claims against Lenovo arise out of the installation of VisualDiscovery on class members’ laptops. For each cause of action, plaintiffs assert the performance, privacy, and security issues created by VisualDiscovery that decreased the value of their laptops:

VisualDiscovery . . . actually and substantially harmed the functioning of the computers by slowing down their internet speeds and reducing their battery life, impairing the computers’ condition, quality, and value. This interference also . . . exposed their private web data to privacy violations and security breaches, thus reducing the condition, quality, and value of the computers for the time period that VisualDiscovery was installed on them.

Compl. ¶¶ 247-49; *see id.* ¶¶ 152-158, 163, 185, 194-97, 207-11, 219-27, 232-34, 240-243, 256-60, 274-76. According to plaintiffs, class members’ “computers suffered a diminution in value during the time period in which VisualDiscovery was installed” and class members “bought computers that they otherwise would not have, overpaid for their computers, [and] did not receive the benefit of their bargain.” *Id.* ¶ 185. Although plaintiffs lack standing to pursue claims on the basis that the SSL hijacker tool exposed their laptops and information to potential security breaches, plaintiffs have established standing to pursue claims based on the alleged privacy and performances problems caused by VisualDiscovery.

Threat of a future security breach is generally too speculative to support standing. In *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, (2013), the Supreme Court found that an “injury based on potential future surveillance” was not “certainly impending” because it was based on a “speculative chain of possibilities,” and therefore could not constitute injury in fact. *Id.* at 1150-51; *see also Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 970 (N.D. Cal. 2015) (“economic injury that rests on the risk presented by an underlying product defect fails to establish injury in fact if the underlying risk is itself speculative”). In this case, however, plaintiffs not only speculate that VisualDiscovery might allow for future hacking by third parties—plaintiffs also allege that the operation of VisualDiscovery—the privacy violations and performance effects it caused—

1 actually decreased the value of their laptops. *See, e.g.*, Compl. ¶¶ 59, 60, 95.

2 Plaintiffs have alleged that VisualDiscovery accessed their computers and intercepted their
3 data, causing injury in fact in the form of reduced performance. *See In re Google Android*
4 *Consumer Privacy Litig.*, No. 11-MD-02264 JSW, 2013 WL 1283236, at *5 (N.D. Cal. Mar. 26,
5 2013) (finding standing where plaintiffs alleged “that their batteries discharged more quickly and
6 that their services were interrupted” by Google’s collection of data); *In re iPhone Application*
7 *Litig.*, 844 F. Supp. 2d 1040, 1054 (N.D. Cal. 2012) (“Plaintiffs have alleged actual injury,
8 including: diminished and consumed iDevice resources, such as storage, battery life, and
9 bandwidth.”).

10 Moreover, with respect to plaintiffs’ consumer protection claims, “when, as here, Plaintiffs
11 contend that class members paid more for a product than they otherwise would have paid, or
12 bought it when they otherwise would not have done so they have suffered an Article III injury in
13 fact.” *Hinojos v. Kohl’s Corp.*, 718 F.3d 1098, 1104 (9th Cir. 2013), *as amended on denial of*
14 *reh’g and reh’g en banc* (July 8, 2013) (addressing UCL, CLRA, and FAL claims) (internal
15 quotation omitted); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1038 (N.D. Cal. 2014)
16 (finding that plaintiffs had standing to bring false advertising claims based on allegations that
17 “Apple misled them through its advertising and failed to disclose material information, that each
18 Plaintiff relied on these misrepresentations or nondisclosures,” and that each class member
19 overpaid for the products); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1056 (N.D. Cal.
20 2012) (finding standing for a variety of claims—including UCL, CLRA, CFAA, negligence, and
21 trespass claims—based on plaintiffs’ allegations that defendant “designed its products to allow
22 consumers’ personal information to be transmitted to third parties” and “led them to overpay for
23 their devices”).

24 The court is not persuaded by Lenovo’s reliance on *In re LinkedIn User Privacy Litigation*,
25 932 F. Supp. 2d 1089 (N.D. Cal. 2013). There, the district court rejected plaintiffs’ overpayment
26 theory of harm because plaintiffs failed to link the alleged injury with the specific claim asserted:

27 Plaintiffs contend that LinkedIn breached the contract by not providing the level of
28 security it allegedly promised to provide. The economic loss Plaintiffs allege—not
receiving the full benefit of the bargain—cannot be the ‘resulting damages’ of this

alleged breach. Rather, this injury could only have occurred at some point before the breach, at the time the parties entered into the contract.

Id. at 1094. The court further found that plaintiffs had not alleged either consideration or reliance in connection with the alleged security promises. *Id.* at 1092-94. In this case, there is no breach of contract claim at issue. Instead, plaintiffs allege that they overpaid for their laptops because reasonable consumers would not expect their laptops to come preinstalled with the software and “would not have purchased the computers or would have paid substantially less for them” if Lenovo had adequately disclosed that Visual Discovery was preinstalled. *Id.* ¶ 184.

Lenovo’s citation to *Birdsong v. Apple, Inc.*, 590 F.3d 955 (9th Cir. 2009) is of only limited value. In *Birdsong*, plaintiffs alleged that their iPods came with “a defect (an inherent risk of hearing loss), which caused their iPods to be worth less than what they paid for them.” 590 F.3d at 961. In the instant case, the alleged “security vulnerabilities” created only a hypothetical risk of harm; third parties would need to exploit the vulnerabilities in order for harm to occur. However, unlike plaintiffs in *Birdsong*, who alleged only a “hypothetical risk of hearing loss” to consumers who might “choose to use their iPods in a risky manner,” 590 F.3d at 961, plaintiffs in the instant case allege that defendants’ privacy violations and the resulting decreased performance actually happened.

B. Statutory Injury

In opposing Lenovo’s motion to dismiss, plaintiffs also claimed Article III standing based on alleged violations of the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, California’s Computer Spyware Act, and California’s Invasion of Privacy Act. After the hearing on Lenovo’s motion, however, the Supreme Court addressed the question of whether an alleged violation of the Fair Credit Reporting Act could satisfy the injury-in-fact requirement. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). Because the court finds that plaintiffs have standing to pursue relief for economic injury on all claims and because the parties have not briefed the question post-*Spokeo*, the court declines to consider whether the statutory violations alleged by plaintiffs are sufficient to establish injury in fact.

III. MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

A motion to dismiss for failure to state a claim under Federal Rule of Civil Procedure

12(b)(6) tests the legal sufficiency of a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). While a complaint need not contain detailed factual allegations, it “must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal citation omitted). “When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief.” *Id.* at 679. However, “the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* (citing *Twombly*, 550 U.S. at 555).

A. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(b)

Lenovo’s motion to dismiss plaintiffs’ CFAA claim is denied. The CFAA creates federal criminal and civil liability for “[f]raud and related activity in connection with computers”—such as intentionally accessing a computer without authorization. 18 U.S.C. § 1030. Section 1030(b) of the CFAA extends liability to anyone who “conspires to commit” such acts. Plaintiffs allege that Lenovo and Superfish “conspired to exceed their authorized access” to plaintiffs’ computers by designing, installing, and operating VisualDiscovery because plaintiffs “did not authorize or consent to Defendants’ interception of Plaintiffs’ communications through VisualDiscovery.” Compl. ¶¶ 155-56.

Lenovo argues that it cannot be subject to CFAA liability because Lenovo was “authorized” to access the laptops in question when Lenovo preinstalled the software. *See Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 983 (D. Colo. 2016) (dismissing CFAA claims, including conspiracy claims, where the primary defendant was “authorized to access the relevant information for at least some purpose at the time of the alleged violation”). But plaintiffs’ CFAA claim is not based on Lenovo’s access during Lenovo’s ownership of the computers; rather, plaintiffs’ allege that Lenovo conspired to enable Superfish to access the

laptops after they were sold to consumers. *See id.* at 984 (denying motion to dismiss § 1030(b) conspiracy claim against a defendant “encouraged” another defendant’s access after authorization had been withdrawn).

Lenovo also argues that plaintiffs do not adequately plead a conspiracy under § 1030(b), which generally requires “specific allegations of an agreement and common activities.” *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 835 (N.D. Cal. 2014) (citing *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285, 1294 (M.D. Fla. 2012); *Vacation Club Servs., Inc. v. Rodriguez*, No. 6:10-CV-247ORL31GJK, 2010 WL 1645129, at *2 (M.D. Fla. Apr. 22, 2010)). In this case, plaintiffs allege that Lenovo entered into an agreement with Superfish to preinstall VisualDiscovery on several laptop models and “share in any revenues that flowed from the partnership.” Compl. ¶ 72. Plaintiffs further allege Lenovo’s “early discussions” with Superfish “included demonstrations of the operation of VisualDiscovery” to senior Lenovo executives, “some of whom expressed concerns” and that Lenovo was “well aware, months before any of its computers were sold with VisualDiscovery loaded, that the program was built on the much-criticized Komodia Redirector and SSL Decoder programs” because Superfish disclosed its use of Komodia code in writing *Id.* ¶¶ 71, 66. Plaintiffs also claim that Lenovo knew, based on its own testing, that VisualDiscovery would negatively impact the laptops once installed. *See id.* ¶¶ 76-77, 79. According to plaintiffs, Lenovo and Superfish agreed to make the installation process as “silent” as possible. *Id.* ¶ 69. Plaintiffs, therefore, allege “facts showing ‘a knowing agreement with another to commit the unlawful act.’” *NetApp*, 41 F. Supp. 3d at 835 (quoting *Trademotion*, 857 F. Supp. 2d at 1294). Lenovo’s citation to *Jung v. Chorus Music Studio, Inc.*, No. 13-CV-1494 CM RLE, 2014 WL 4493795 (S.D.N.Y. Sept. 11, 2014) in unavailing. In that case, the counterclaimants failed to allege that the defendants had “any connection” to the alleged violation. 2014 WL 4493795, at *7.

Finally, Lenovo argues that no named plaintiff suffered the statutory minimum loss. To maintain a civil cause of action against Lenovo, plaintiffs must plead a “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” 18 U.S.C.

§ 1030(c)(4)(A)(i)(I). “[L]oss’ means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). Plaintiff John Whittle alleges that he used his Lenovo for his income tax preparation business and suffered losses “as a result of computer performance issues and suspected privacy intrusions caused by VisualDiscovery.” Compl. ¶ 150. Specifically, Mr. Whittle alleges that the “revenue lost, costs incurred, and consequential damages suffered because of interruption of service immediately before the federal and state income tax deadline of April 15, 2015, exceeds \$5,000.” *Id.* While these allegations are not particularly detailed, “for the purposes of deciding a motion to dismiss pursuant to Rule 12(b)(6), the issue is not whether a party will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims.” *Jung*, 2014 WL 4493795, at *7 (internal quotation marks omitted) (finding allegations that counterclaimant “spent at least \$5,000 to respond to the theft and assess the damage within the meaning of the CFAA” sufficient). The court concludes, therefore, that plaintiff John Whittle adequately alleges the minimum statutory loss. *Cf. Volk v. Zeenah*, No. 608CV094, 2010 WL 318261, at *3 (S.D. Ga. Jan. 25, 2010) (granting leave to amend because plaintiff’s new allegations of losses attributable to increased server traffic, diagnosing data breach, and installing a new server “would seem to salvage” plaintiff’s CFAA claim).

B. California’s Computer Crime Law, Cal. Penal Code § 502

Lenovo’s motion to dismiss plaintiffs’ Computer Crime Law claim is denied. Lenovo argues that plaintiffs’ Computer Crime Law claim should be dismissed for the same reasons that plaintiffs’ CFAA claim should be dismissed. *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014) (“necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA”). Lenovo’s motion to dismiss plaintiffs’ CFAA claim, however, is denied, and Lenovo does not move to dismiss plaintiffs’ Computer Crime Law claim on any other basis.

C. Electronic Communications Privacy Act, 18 U.S.C. § 2512

Lenovo's motion to dismiss plaintiffs' ECPA claim is granted. Lenovo argues that plaintiffs' ECPA claim should be dismissed because plaintiffs have failed to allege that Lenovo—as opposed to Superfish—"intercepted" or "acquired" any of plaintiffs' communications.

Plaintiffs argue that the ECPA claim asserted against Lenovo is not brought under § 2511—which prohibits the "[i]nterception and disclosure of wire, oral, or electronic communications," but rather under § 2512—which prohibits the "[m]anufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices." Lenovo expresses surprise at plaintiffs' response: "Plaintiffs retreat to a corner of the Wiretap Act, 18 U.S.C. § 2512, and then argue that Lenovo did not go into that specific corner, thereby waiving its Wiretap Act arguments. This is ludicrous." Dkt. No. 108 at 4. The court cannot agree that plaintiffs are retreating. Count II of plaintiffs' complaint cites 18 U.S.C. § 2512 in the subtitle. In the paragraphs under the Count II heading, plaintiffs reference § 2512 three more times and allege that "Lenovo and Superfish intentionally possessed, manufactured, sold, and/or assembled" a device "primarily useful for the purpose of the surreptitious interception of wire or electronic communications." Compl. ¶¶ 160-165.

Section 2512, however, does not establish a private right of action—it addresses only criminal liability. Under § 2520(a) of the ECPA, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation" of the chapter "may recover in a civil action from the person or entity . . . which *engaged in that violation*." 18 U.S.C. § 2520 (emphasis added). Thus, "Congress chose to confine private civil actions to defendants who had 'intercepted, disclosed, or intentionally used [a communication] in violation of . . . chapter [119 of title 18.]'" *DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1127 (11th Cir. 2004) (quoting 18 U.S.C. § 2520(a)); *see also DirecTV Inc. v. Nicholas*, 403 F.3d 223, 227 (4th Cir. 2005) ("express language of § 2520 is therefore not susceptible to a construction which would provide a cause of action against one who manufactures or sells a device in violation of § 2512 but does not engage in conduct violative of § 2511"); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th

Cir. 2000) (“Section 2520(a)’s plain, unambiguous language authorizes a civil action by one whose covered ‘communication is *intercepted, disclosed, or intentionally used in violation of this chapter,*’ from ‘the person or entity *which engaged in that violation.*”); *In re Cases Filed by DirecTV, Inc.*, 344 F. Supp. 2d 636, 644 (D. Ariz. 2004) (“The plain language of 18 U.S.C. § 2520(a) thus creates a private right of action against a person who ‘intercepted, disclosed, or intentionally used’ a wire, oral, or electronic communication . . . ,” but “does not ‘create a private right of action for the manufacture, assembly, or sale of a device in violation of § 2512(1)(b).’”). Plaintiffs do not allege that Lenovo intercepted, disclosed, or intentionally used any of their communications and therefore cannot assert a claim based on violation of § 2512.

Plaintiffs argue that Lenovo should not be permitted to challenge the ECPA claim under § 2512 because Lenovo did not address § 2512 in its motion. While Lenovo could have been more precise in its opening brief, Lenovo did argue that plaintiffs failed to allege that Lenovo intercepted any communications as required for civil liability under any section of the ECPA. *See* Dkt. No. 98-1 at 11. Plaintiffs’ § 2512 claim against Lenovo, therefore, is dismissed.

D. California Invasion of Privacy Act, Cal. Penal Code § 631

Lenovo’s motion to dismiss plaintiffs’ CIPA claim is denied. Lenovo argues that analysis for a violation of CIPA is the same that under the ECPA. *See NovelPoster*, 140 F. Supp. 3d at 954 (“analysis for a violation of CIPA is the same as that under the federal Wiretap Act”). As plaintiffs point out, however, CIPA provides for recovery against anyone “who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things” prohibited by the statute. Cal. Penal Code § 631; *see also* Cal. Penal Code § 637.2 (“[a]ny person who has been injured by a violation of this chapter may bring an action against the person who committed the violation”). In this case, plaintiffs claim that “Lenovo aided, agreed with, or conspired with Superfish” to violate CIPA. Compl. ¶233.

E. California’s Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947

Lenovo’s motion to dismiss plaintiffs’ Spyware Act claim is granted. California’s

Computer Spyware Act prohibits anyone “who is not an authorized user, as defined in Section 22947.1,” from causing “computer software to be copied onto the computer of a consumer” and using that software for certain purposes. Cal. Bus. & Prof. Code § 22947.2-3. “‘Authorized user,’ with respect to a computer, means a person who owns or is authorized by the owner or lessee to use the computer.” Cal. Bus. & Prof. Code § 22947.1. Plaintiffs do not dispute that Lenovo owned the laptops when it preinstalled VisualDiscovery. *See, e.g.*, Compl. ¶ 80 (“Lenovo began shipping hundreds of thousands of computers to consumers in the United States with VisualDiscovery hidden away deep within the operating system.”). Therefore, Lenovo was an “authorized user” within the meaning of the statute. Plaintiffs argue that liability should extend to Lenovo’s installation of software on computers that Lenovo later sold to consumers, but the plain language of the statute is limited to installation by “unauthorized” users.

F. Trespass to Chattels Claims

Lenovo’s motion to dismiss plaintiffs’ trespass to chattels claims under both California and New York law is denied. In California, trespass to chattels “lies where an intentional interference with the possession of personal property has proximately caused injury.” *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566 (1996). The elements are very similar under New York law. *See Biosafe-One, Inc. v. Hawks*, 639 F. Supp. 2d 358, 368 (S.D.N.Y. 2009), *aff’d*, 379 F. App’x 4 (2d Cir. 2010) (citing *Sweeney v. Bruckner Plaza Assocs. LP*, 875 N.Y.S.2d 824 (Sup. Ct. 2004), *aff’d*, 799 N.Y.S.2d 483 (N.Y. App. Div. 2005)) (plaintiffs must prove that “(1) defendants acted with intent, (2) to physically interfere with (3) plaintiffs’ lawful possession, and (4) harm resulted”). In this case, plaintiffs contend that Lenovo, through the installation of VisualDiscovery, interfered with plaintiffs’ use of their computers and “actually and substantially harmed the functioning of the computers by slowing down their internet speeds and reducing their battery life, impairing the computers’ condition, quality, and value.” Compl. ¶¶ 247-49; 274-76.

Lenovo relies on *In re iPhone Application Litigation*, in which plaintiffs alleged that unwanted apps “consumed portions of the cache and/or gigabytes of memory on their devices” and used “valuable bandwidth and storage space” on plaintiffs’ devices. 844 F. Supp. 2d at 1069. The

district court dismissed plaintiffs' trespass to chattels claim, finding that while plaintiffs' "allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass." *Id.* In contrast, plaintiffs in the instant case plausibly allege that the "operation of VisualDiscovery significantly degraded the performance of the Lenovo computers." Compl. ¶ 59. Plaintiffs describe VisualDiscovery as running "constantly," and allege that while VisualDiscovery was operational, it decreased battery life, "slowed internet upload speeds by as much as 55 percent and download speeds by as much as 16 percent," and "caused certain webpages to fail to load correctly or not load at all." *Id.* ¶¶ 4, 59. Plaintiffs allege that consumers complained that VisualDiscovery "interfered with watching videos online, caused the computers to run slow, blocked or slowed connections to certain websites, and caused security issues." *Id.* ¶ 95.

Accepting plaintiffs' allegations as true for purposes of Lenovo's motion to dismiss, the court is satisfied that plaintiffs have alleged some measureable loss based on the installation of VisualDiscovery. *See Sch. of Visual Arts v. Kuprewicz*, 771 N.Y.S.2d 804, 808 (Sup. Ct. 2003) (finding plaintiffs' allegations that "large volumes" of unsolicited job applications and pornographic e-mails "depleted hard disk space, drained processing power, and adversely affected other system resources on SVA's computer system" sufficient); *Thrifty-Tel*, 46 Cal. App. 4th at 1564 (finding claim actionable where defendant's automated dialing system "overburdened the system, denying some subscribers access to phones lines"); *cf. Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1357 (2003) ("That Hamidi's messages temporarily used some portion of the Intel computers' processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system.").

G. Negligence Claims

Plaintiff's negligence claims under New York and California law are dismissed as barred by the economic loss rule. "Simply stated, the economic loss rule provides: Where a purchaser's expectations in a sale are frustrated because the product he bought is not working properly, his

remedy is said to be in contract alone, for he has suffered only ‘economic’ losses.” *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) (citation omitted). “This doctrine hinges on a distinction drawn between transactions involving the sale of goods for commercial purposes where economic expectations are protected by commercial and contract law, and those involving the sale of defective products to individual consumers who are injured in a manner which has traditionally been remedied by resort to the law of torts.” *Id.* In economic loss cases, “the damaged party has lost part of its bargain and the parties are relegated to the contractual remedies they negotiated, including warranties governing the rights and obligations between manufacturers and suppliers of goods. In contrast, tort liability is generally present where personal injury and other property damage is at issue.” *Bristol Vill., Inc. v. La.-Pac. Corp.*, 916 F. Supp. 2d 357, 365 (W.D.N.Y. 2013) (internal quotation marks and citations omitted).

Plaintiffs contend that the economic loss rule does not necessarily bar tort recovery for damage to portions of a larger product into which a defective product component is incorporated, citing *Jimenez v. Superior Court*, 29 Cal. 4th 473, 476 (2002) (allowing strict liability tort claim against window manufacturer where defective window damaged other parts of house in which window was installed) and *Adirondack Combustion Tech., Inc. v. Unicontrol, Inc.*, 793 N.Y.S.2d 576 (N.Y. App. Div. 2005) (allowing tort claims against manufacturer of boiler controller device where controller device caused damage to boiler). Plaintiffs contend that their “computers constitute ‘other property’ injured by VisualDiscovery,” so the economic loss rule does not apply. Dkt. No. 106 at 20. The court is not persuaded by this argument because plaintiffs seek to recover from the laptop manufacturer because their laptops do not work properly—which is precisely the kind of recovery barred by the economic loss rule.

Under New York law, tort recovery is not available “to a downstream purchaser where the claimed losses flow from damage to the property that is the subject of the contract.” *Bocre Leasing Corp. v. Gen. Motors Corp. (Allison Gas Turbine Div.)*, 645 N.E.2d 1195, 1199 (N.Y. 1995). “Notably, recovery for damage caused to a unit or system by a defective component has been consistently barred by the economic loss rule, even where that defective component was

1 manufactured by a third party.” *Bristol*, 916 F. Supp. 2d at 365 (citing cases). Plaintiffs’ citation to
 2 *Adirondack Combustion* is inapposite; plaintiff there—unlike plaintiffs in the instant case—
 3 claimed damage to a product other than the product supplied by the manufacturer. 793 N.Y.S.2d at
 4 579 (2005) (finding economic loss argument “flawed” because “defendant’s product was the
 5 controller device, not the boiler, which sustained direct and consequential physical damage as a
 6 result of . . . the failure of defendant’s product”).

7 Nor does plaintiffs’ California case support their position. In *Jimenez*, the California
 8 Supreme Court permitted a tort action against the manufacture of a defective window for harm
 9 that the window caused to a house. 29 Cal. 4th at 484-485. Plaintiffs, by analogy, would likely be
 10 permitted to pursue tort claims against Superfish for damage that VisualDiscovery caused to other
 11 property—namely plaintiffs’ Lenovo laptops—in which the software was installed. But nothing in
 12 *Jimenez* permits plaintiffs to pursue tort recovery against a laptop manufacturer for damage caused
 13 to the laptops.

14 **H. New York Consumer Protection Claim, N.Y. Gen. Bus. Law § 349**

15 Lenovo’s motion to dismiss plaintiffs’ GBL claim is granted. Under section 349, a plaintiff
 16 seeking to recover damages must be able to prove that “a material deceptive act or practice *caused*
 17 *actual, although not necessarily pecuniary, harm.*” *Small v. Lorillard Tobacco Co.*, 94 N.Y.2d 43,
 18 56 (1999) (emphasis in original). Plaintiffs claim that, as a result of Lenovo’s deceptive acts and
 19 practices, they “received computers less than they bargained for and have spent money to remove
 20 VisualDiscovery and obtain antivirus software.” Compl. ¶ 260.

21 The New York Court of Appeals has rejected the argument that “consumers who buy a
 22 product that they would not have purchased, absent a manufacturer’s deceptive commercial
 23 practices” have necessarily suffered an injury for GBL purposes. *Small*, 94 N.Y.2d at 56; *see also*
 24 *Gomez-Jimenez v. N.Y. Law Sch.*, 943 N.Y.S.2d 834, 849 (Sup. Ct.), *aff’d*, 103 A.D.3d 13, 956
 25 N.Y.S.2d 54 (2012) (“benefit-of-the-bargain damages must be based on the bargain that was
 26 actually struck, not on a bargain whose terms must be supplied by hypotheses about what parties
 27 would have done if the circumstances surrounding their transaction had been different”) (quoting

Barrows v. Forest Labs., Inc., 742 F.2d 54 (2d Cir. 1984)). Plaintiffs, therefore, cannot rely on their overpayment theory to establish injury for purposes of their section 349 claim. *See, e.g., Baron v. Pfizer, Inc.*, 840 N.Y.S.2d 445, 448 (N.Y. App. Div. 2007) (finding that plaintiff failed alleged to allege a “cognizable injury” where she claimed that “she would not have purchased the drug absent defendant’s deceptive practices”). The cases cited by plaintiffs do not support their position that a theory of overpayment is enough by itself. In *Bildstein v. MasterCard Int’l, Inc.*, No. 03 CIV.9826I(WHP), 2005 WL 1324972 (S.D.N.Y. June 6, 2005), plaintiff alleged that he was charged an undisclosed foreign currency transaction fee that he could have otherwise avoided. *Id.* at *4. Plaintiffs here do not allege that they were charged any fee in connection with the installation of VisualDiscovery. In *Tomassini v. FCA U.S. LLC*, No. 3:14-CV-1226 MAD/DEP, 2015 WL 3868343 (N.D.N.Y. June 23, 2015), defendant did not dispute that plaintiff had “adequately pleaded injury caused by defendant’s alleged pre-sale omissions regarding a product defect.” *Id.* at *8.

Plaintiffs also rely on the assertion that they were forced to spend money to remove VisualDiscovery. Here, however, plaintiffs run into a standing problem. Only one named plaintiff, John Whittle, specifically alleges that he spent money to remove the software. *See* Compl. ¶ 150. Mr. Whittle, however, is a resident of Arizona, not New York, *id.* ¶ 12, and while plaintiffs allege that “Lenovo’s direct sales to consumers are governed by a uniform sales agreement that includes a New York choice-of-law provision,” *id.* ¶ 122, Mr. Whittle claims to have purchased his laptop indirectly—“through Ebay.com,” *id.* ¶ 12. Plaintiffs cannot maintain a New York consumer protection claim without plausibly alleging that at least one named plaintiff has standing to pursue relief.

I. California Consumer Protection Claims Under UCL and CLRA

Lenovo’s motion to dismiss plaintiffs’ fraudulent omissions claims under California law is denied. The UCL prohibits “any unlawful, unfair or fraudulent business act.” Cal. Bus. & Prof. Code § 17200. The CLRA prohibits “unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services

to any consumer.” Cal. Civ. Code § 1770. Plaintiffs’ claims under the UCL’s “unfair” and “fraudulent” prongs and the CLRA are fraudulent omissions claims based on Lenovo’s alleged failure to disclose the installation of VisualDiscovery. *See* Compl. ¶¶ 184, 192.² The court is not convinced by any of Lenovo’s statute-specific arguments for dismissal, nor is the court persuaded by Lenovo’s argument that plaintiffs cannot allege a fraudulent omission.

1. UCL Claims

Lenovo argues that plaintiffs’ UCL claims must fail because plaintiffs did not lose money or property, because an adequate remedy at law exists, and because disgorgement is not available with respect to the profits Lenovo earned from Superfish. As previously discussed, plaintiffs have adequately alleged economic harm, which satisfies the UCL’s “lost money or property” requirement. *See Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011) (noting that there are “innumerable ways in which economic injury from unfair competition may be shown,” including through allegations that a plaintiff “surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have”). Plaintiffs do not appear to seek disgorgement of the money paid from Superfish and are permitted to plead remedies in the alternative. Therefore, the court finds that “questions about the appropriateness of specific remedies are premature at this stage of the litigation.” *James ex rel. James Ambrose Johnson, Jr. 1999 Trust v. UMG Recordings*, No. C 11-1613 SI, 2011 WL 5192476, at *5 (N.D. Cal. Nov. 1, 2011).

2. CLRA Claim

Lenovo argues that plaintiffs’ CLRA claim must fail “because software is neither a ‘good’ nor a ‘service’ covered by the CLRA.” *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1070. But plaintiffs do not bring a claim based on deceptive practices in connection with the sale or lease of VisualDiscovery. Rather, their CLRA claim is premised on their purchase of Lenovo laptops.

² Lenovo also moves to dismiss plaintiffs’ UCL’s “unlawful” prong claim, which is predicated on all other claims asserted in the complaint. *See* Compl. ¶ 183. Plaintiffs’ “unlawful” prong claim survives to the extent that plaintiffs’ other claims survive Lenovo’s motion to dismiss.

1 *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1071 (finding that plaintiffs “articulated a
 2 damages claim that is cognizable under the CLRA” by alleging that if “Apple disclosed the true
 3 cost of the purportedly free Apps . . . the value of the iPhones would have been materially less
 4 than what Plaintiffs paid.”) (alteration in original). Therefore, Lenovo’s motion dismiss plaintiffs’
 5 CLRA claim is denied.

6 **3. Fraudulent Omissions**

7 Lenovo argues that no one could have been deceived by its failure to disclose the
 8 installation of VisualDiscovery. Plaintiffs, however, claim that Lenovo violated a “duty to disclose
 9 the pre-installation of VisualDiscovery and its associated privacy risks and computer performance
 10 issues because Lenovo had exclusive knowledge of the pre-installation.” *Id.* ¶ 194 Plaintiffs allege
 11 that, as a result of these fraudulent omissions, they were deceived into overpaying for their
 12 laptops. *Id.* ¶ 195-97, 184-85.

13 **a. Duty to Disclose**

14 Lenovo argues that plaintiffs cannot allege a duty to disclose because a “manufacturer’s
 15 duty to consumers is limited to its warranty obligations absent either an affirmative
 16 misrepresentation or a safety issue.” *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1141 (9th
 17 Cir. 2012) (quoting *Oestreicher v. Alienware Corp.*, 322 F. App’x 489, 493 (9th Cir. 2009)); *see*
 18 *also Opperman*, 87 F. Supp. 3d at 1052 (dismissing omissions claims based on Apple’s
 19 “affirmative duty to disclose material facts of which it had exclusive knowledge, *i.e.*, the
 20 vulnerability of Plaintiffs’ iDevices to the theft of their address books by third party apps,”
 21 because plaintiffs failed to identify either an affirmative representation or safety issue).

22 Plaintiffs do not allege any affirmative misrepresentation or safety issue in this case.
 23 Instead, plaintiffs cite cases finding a duty to disclose absent either circumstance, but where the
 24 defendant was alleged to have exclusive knowledge of material information. *See Norcia v.*
 25 *Samsung Telecommunications Am., LLC*, No. 14-CV-00582-JD, 2015 WL 4967247, at *6 (N.D.
 26 Cal. Aug. 20, 2015) (rejecting “defendants’ argument that Samsung’s duty to disclose here was
 27 limited to defects relating to safety concerns” and denying motion to dismiss omissions claim
 28

where “benchmarking manipulations were within Samsung’s exclusive knowledge and therefore subject to a duty to disclose”); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1112 (N.D. Cal. 2015) (denying motion to dismiss omissions claims where plaintiff alleged that defendant had a duty “to disclose the existence and functionality” of Carrier IQ Software because defendant had “exclusive knowledge”); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1231 (N.D. Cal. 2014) (denying motion to dismiss where plaintiffs alleged “that Adobe had exclusive knowledge of the fact that its security practices fell short of industry standards” and therefore had a duty to disclose).

This court must apply California law. In *Wilson*, cited by Lenovo, the Ninth Circuit noted that California federal courts have generally interpreted *Daugherty*, a California Court of Appeal decision, as limiting a manufacturer’s duty to disclose “to its warranty obligations absent either an affirmative misrepresentation or a safety issue.” 668 F.3d at 1141 (citing *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824 (2006), *as modified* (Nov. 8, 2006)). In *Norcia*, cited by plaintiffs, the district court noted that “the California Court of Appeal itself has very recently clarified that this is a misreading of California law.” 2015 WL 4967247, at *6 (citing *Rutledge v. Hewlett-Packard Co.*, 238 Cal. App. 4th 1164, 1174 (2015), *as modified on denial of reh’g* (Aug. 21, 2015)). In *Rutledge*, the California Court of Appeal explained that *Daugherty* decision itself addressed the “disclosure of defects related to safety concerns in the context of CLRA and UCL,” but that nothing in *Daugherty* precludes the existence of “a duty to disclose material information known to a manufacturer and concealed from a consumer” in the absence of safety concerns. 238 Cal. App. 4th at 1174 (finding that plaintiffs had stated a fraudulent omissions claim by alleging that HP concealed “the material fact that HP notebook computers have known defects that cause display problems”).

Lenovo argues that *Wilson* should control, but the Ninth Circuit has indicated that its own precedents are “only binding in the absence of any subsequent indication from the California courts that [the Ninth Circuit’s] interpretation was incorrect.” *In re Watts*, 298 F.3d 1077, 1083 (9th Cir. 2002) (quoting *Owen ex rel. Owen v. United States*, 713 F.2d 1461, 1464 (9th Cir. 1983))

(adopting state appellate court’s interpretation of state law over prior interpretation by Ninth Circuit). In the “absence of a pronouncement by the highest court of a state,” if a recent decision from a state court of appeal casts “new light on the question,” this court must follow the court of appeal’s decision “unless there is convincing evidence that the highest court of the state would decide differently.” *Watts*, 298 F.3d at 1083 (9th Cir. 2002) (quoting *Owen*, 713 F.2d at 1464) (emphasis omitted).

No clear and convincing evidence suggests that the California Supreme Court would decide *Rutledge* differently. As explained in *Rutledge*, the California Court of Appeal’s earlier *Daugherty* decision does not explicitly foreclose the possibility of a duty to disclose absent an affirmative representation or safety concern. Accordingly, the court declines to dismiss plaintiffs’ UCL and CLRA claims for failure to allege either an affirmative misrepresentation or a safety concern.

b. Exclusive Knowledge of Material Facts

Lenovo’s next argument—that plaintiffs do not adequately allege Lenovo’s exclusive knowledge—is not well-taken. Plaintiffs allege that “Lenovo and Superfish agreed that the installation process for VisualDiscovery would be ‘as silent as we can make it,’ . . . installed at the lowest level of the operating system.” Compl. ¶ 69. Plaintiffs further allege that Lenovo knew how the software worked and that its own testing revealed the performances problems, but that Lenovo began shipping the laptops anyway. Compl. ¶¶ 71, 79-80, 96. These facts are sufficient to allege Lenovo’s exclusive knowledge. *See, e.g., Norcia*, 2015 WL 4967247, at *7 (finding that plaintiffs had adequately alleged exclusive knowledge of software functionality because even publicly-available source code may not be “easily accessible or understandable to the average consumer”); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1112 (finding allegations that “only defendants knew of the installation and functionality” of the software sufficient to plead exclusive knowledge).

Lenovo also argues that no consumer could be materially misled by its failure to disclose. Plaintiffs, however, have identified the content that should have been disclosed—that VisualDiscovery was installed and that it would collect plaintiffs’ browsing information and

decrease the performance of their laptops. “‘A fact is deemed material, and obligates an exclusively knowledgeable defendant to disclose it, if a reasonable consumer would deem it important in determining how to act in the transaction at issue.’” *In re Adobe*, 66 F. Supp. 3d at 1229 (quoting *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 256 (2011), *as modified* (Dec. 28, 2011)) (internal quotation marks and alterations omitted). Here, plaintiffs allege that “a reasonable purchaser would not anticipate that the computers would be installed with such software” and that plaintiffs would not have purchased or would have paid less for the laptops had they known. Compl. ¶¶ 193, 184. These allegations are sufficient to plead the materiality of the omissions. *See In re Carrier IQ*, 78 F. Supp. 3d at 1113 (finding that plaintiffs “alleged materiality by alleging that had they been aware of the installation and functionality of the Carrier IQ Software, they would not have purchased their mobile devices”).

Lenovo’s citation to *Lee v. Toyota Motor Sales, U.S.A., Inc.*, 992 F. Supp. 2d 962 (C.D. Cal. 2014) is not persuasive. In *Lee*, the court dismissed plaintiffs’ omissions claims because plaintiffs “failed to allege any facts demonstrating that the PCS is ‘defective,’ or, if it was, that Toyota was aware that it was defective at the time Plaintiffs purchased their vehicles.” *Id.* at 975. As noted above, plaintiffs in the instant case have alleged the problems caused by VisualDiscovery and Lenovo’s exclusive knowledge. The other cases cited by Lenovo are inapposite because they do not address sufficient pleading for an omissions claim. In *Norcia*, the district court dismissed plaintiff’s claims that Samsung had affirmatively misrepresented storage capacity because plaintiff did not plausibly allege “what statement was false and why.” 2015 WL 4967247, at *8. And in *Derbaremdiker v. Applebee’s Int’l, Inc.*, No. 12-CV-01058 KAM, 2012 WL 4482057 (E.D.N.Y. Sept. 26, 2012), *aff’d*, 519 F. App’x 77 (2d Cir. 2013), the court found that a reasonable consumer would not be misled about sweepstakes odds because the receipt, which was not misleading on its face, directed consumers to defendant’s website for the official rules. *Id.* at *5-6.

J. Injunctive Relief

Lenovo’s motion to dismiss plaintiffs’ claim for injunctive relief is granted as unopposed.

Lenovo notes that several allegations in the complaint suggest that plaintiffs may seek injunctive relief, although plaintiffs do not list injunctive relief in the complaint's prayer for relief. Plaintiffs do not address the availability of injunctive relief in their opposition.

IV. MOTION FOR CLASS CERTIFICATION

Plaintiffs seek to certify three classes of purchasers:

Direct Purchaser Class (represented by Richard Krause and Robert Ravencamp): All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in the United States directly from Lenovo.

Indirect Purchaser Class (represented by Jessica Bennett, Rhonda Estrella and John Whittle): All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in the United States from someone other than Lenovo.

California Class (represented by Jessica Bennett and Rhonda Estrella): All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in California.

Plaintiff also seeks the appointment of Pritzker Levine LLP, Girard Gibbs LLP, and Cotchett, Pitre & McCarthy, LLP as class counsel.

As a threshold matter, the court addresses Lenovo's objections to plaintiffs' reply evidence. As a general rule, new evidence presented in a reply should not be considered without giving the non-movant an opportunity to respond. *See Provenz v. Miller*, 102 F.3d 1478, 1483 (9th Cir. 1996). Plaintiffs submitted declarations from Adi Pinhas, the former CEO of Superfish, and both of plaintiffs' damages experts. Plaintiffs contend that these declarations are permissible rebuttal, rather than new evidence. *See Netlist Inc v. Diablo Techs. Inc.*, No. 13-CV-05962-YGR, 2015 WL 153724, at *1 n.1 (N.D. Cal. Jan. 12, 2015). Having reviewed the declarations at issue, the court finds that the Pinhas declaration does not rebut the contents of the Lee declaration, but rather contains new evidence of Lenovo's knowledge that could have been included with plaintiffs' motion. The expert declarations, however, address only the opinions expressed by Lenovo's damages expert and therefore may appropriately be considered as rebuttal evidence.

Before certifying a class, the trial court must conduct a 'rigorous analysis' to determine whether the party seeking certification has met the prerequisites of Rule 23." *Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581, 588 (9th Cir. 2012) (quoting *Zinser v. Accufix Research Inst., Inc.*,

253 F.3d 1180, 1186, *amended* 273 F.3d 1266 (9th Cir. 2001)). In addition, district courts in this circuit have found an implied requirement that the proposed class be ascertainable. *See, e.g., Bias v. Wells Fargo & Co.*, 312 F.R.D. 528, 534 (N.D. Cal. 2015). “A party seeking class certification must affirmatively demonstrate his compliance with the Rule—that is, he must be prepared to prove that there are *in fact* sufficiently numerous parties, common questions of law or fact, etc.” *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011); *see also United Steel, Paper & Forestry, Rubber, Mfg. Energy, Allied Indus. & Serv. Workers Int’l Union, AFL-CIO, CLC v. ConocoPhillips Co.*, 593 F.3d 802, 807 (9th Cir. 2010) (“party seeking class certification bears the burden of demonstrating that the requirements of Rules 23(a) and (b) are met”).

A. Rule 23(a) Requirements

Under Rule 23(a), a plaintiff must demonstrate numerosity, commonality, typicality and adequacy of representation in order to maintain a class. Fed. R. Civ. P. 23(a)(1)-(4). Lenovo does not challenge plaintiffs’ showing with respect to Rule 23(a)’s numerosity requirement. The court addresses Lenovo’s arguments as to the adequacy of representation in the context of typicality because Lenovo’s arguments address whether named plaintiffs’ claims are “reasonably coextensive with those of absent class members,” rather than whether the named plaintiffs have “any conflicts of interest with other class members” or whether they will “prosecute the action vigorously on behalf of the class.” *Staton v. Boeing Co.*, 327 F.3d 938, 957 (9th Cir. 2003).

1. Commonality

Rule 23(a)(2) requires “questions of law or fact common to the class.” Fed. R. Civ. P. 23(a)(2). Lenovo asserts that not all putative class members have standing to assert claims because not “all purchasers” of Lenovo experienced the negative effects of VisualDiscovery.³ The court is not persuaded that the proposed classes are overbroad.

“‘[N]o class may be certified that contains members lacking Article III standing,’ which

³ Lenovo also argues that no class members have suffered any injury at all because plaintiffs do not allege a hacking incident or misuse of plaintiffs’ private information. Plaintiffs’ claims, however, do not rely on such events as the source of harm.

means “it must be possible that class members have suffered injury.” *Torres v. Mercer Canyons Inc.*, No. 15-35615, 2016 WL 4537378, at *8 n. 6 (9th Cir. Aug. 31, 2016) (quoting *Mazza*, 666 F.3d at 594) (noting that class members need not prove such injury at class certification stage). Lenovo argues that the proposed classes include unharmed persons because some number of purchasers (1) liked their computers and gave them positive performance reviews, (2) opted out of or uninstalled VisualDiscovery, and/or (3) did not purchase their Lenovo laptops until after the Superfish servers were shut down in January 2015.⁴

Neither the favorable laptop performance reviews, nor the decision of some class members to opt out or uninstall VisualDiscovery, defeat the commonality of the proposed classes. These circumstances “merely highlight[] the possibility that an injurious course of conduct may sometimes fail to cause injury to certain class members” who were exposed to the conduct. *Torres*, 2016 WL 4537378, at *7. “[E]ven a well-defined class may inevitably contain some individuals who have suffered no harm as a result of a defendant’s unlawful conduct.” *Id.*

The January 2015 server shut down does not defeat commonality of standing because plaintiffs have submitted evidence that VisualDiscovery was operating on the laptops even after the Superfish servers were turned off. *See* Levine Decl., Ex. 36. While Lenovo may have competing evidence to show that no class members suffered harm after a certain point in time, this court examines the merits of plaintiffs’ claims only as to “whether common questions exist; not to determine whether class members could actually prevail.” *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 983 (9th Cir. 2011).

The cases cited by Lenovo are not persuasive because the classes found to be overbroad included “individuals who could not have been injured by [the] alleged wrongful conduct as a matter of law.” *Moore v. Apple Inc.*, 309 F.R.D. 532, 543 (N.D. Cal. 2015); *see also, e.g., Opperman v. Path, Inc.*, No. 13-CV-00453-JST, 2016 WL 3844326, at *13 (N.D. Cal. July 15, 2016) (“a plaintiff who did not sign in to the Path App could not have had her contacts uploaded,

⁴ Lenovo also argues that some purchasers returned their laptops for a refund, but such persons would not fall within the definition of “purchasers” after returning their laptops.

and there was no possibility of injury”). In this case, all class members were exposed to the same disclosure—that is no disclosure at all—and purchased the allegedly defective product. Although all class members may not prevail on the merits of their claims, plaintiffs’ proposed classes do not include members “who, by definition, *could not* have been injured.” *Moore*, 309 F.R.D. at 542.

2. Typicality

A class representative’s claims and defenses must be “typical of the claims or defenses of the class.” Fed. R. Civ. P. 23(a)(3). “Under the Rule’s permissive standards, representative claims are ‘typical’” if they are reasonably coextensive with those of absent class members; they need not be substantially identical.” *Torres*, 2016 WL 4537378, at *11 (quoting *Parsons*, 754 F.3d at 685). “Measures of typicality include ‘whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct.’” *Id.* (quoting *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992)). Here, the court is persuaded that the claims of both the named and unnamed plaintiffs arise out of the same course of conduct—namely the installation of VisualDiscovery. Lenovo has not identified any circumstances that would make named plaintiffs’ claims atypical or subject them to unique defenses.

Lenovo claims that John Whittle never had VisualDiscovery installed on his laptop, citing evidence that Mr. Whittle purchased a refurbished machine with an unknown history and that Mr. Whittle could not say with certainty at his deposition that VisualDiscovery was installed. Mr. Whittle, on the hand, relies on evidence that Lenovo was installing and selling laptops with VisualDiscovery at the time Mr. Whittle’s laptop was manufactured and sold, as well as his own deposition testimony about the performance issues he experienced. The evidence may ultimately establish that Mr. Whittle did not purchase a laptop with VisualDiscovery, but Mr. Whittle submits evidence that he did. This is sufficient at the class certification stage.

Lenovo claims that Richard Krause and Robert Ravencamp cannot represent the class because they had the updated version of VisualDiscovery installed, which Lenovo contends removed the security vulnerability created by SSL hijacker from the software. The court has

determined that plaintiffs’ lack standing to pursue claims based on the security vulnerability.⁵ With respect to plaintiffs’ claims based on the privacy and performance effects of the software, plaintiffs submit expert evidence that the both versions of operated in substantially the same way. *See e.g.*, Levine Decl., Ex. 44 ¶¶ 33-34.

Lenovo claims that the named plaintiffs are not typical because they used their laptops for business purposes, rather than for personal use, while VisualDiscovery was intended for installation on personal use laptops. It is not clear how this distinction would affect plaintiffs’ claims, but in any case, plaintiffs cite evidence that all named plaintiffs used their laptops for personal use at least some of the time. *See* Levine Decl., Ex. 39 at 1; Levine Reply Decl., Ex. 4 (73:21-74:2); Ex. 5 (28:17-29:5); Ex. 6 (18:1-4, 25:10-19); Ex. 7 (46:16-22). Moreover, to the extent Lenovo claims that the named plaintiffs’ claims are atypical because plaintiffs’ experiences with their laptops varied, such circumstances go “to the extent of their damages and not whether named [plaintiffs] ‘possess the same interest and suffer[ed] the same injury as the class members.’” *Wolin v. Jaguar Land Rover N. Am., LLC*, 617 F.3d 1168, 1175 (9th Cir. 2010) (quoting *E. Texas Motor Freight Sys. Inc. v. Rodriguez*, 431 U.S. 395, 403 (1977)).

B. Ascertainability Requirement

To establish ascertainability for class certification purposes, plaintiffs must demonstrate that “members of the proposed class are readily identifiable by objective criteria, and it is administratively feasible to determine whether a particular person is a member of the class.” *Bias*, 312 F.R.D. at 538 (citing *Xavier v. Philip Morris USA Inc.*, 787 F. Supp. 2d 1075, 1089 (N.D. Cal. 2011)). Lenovo does not challenge the ascertainability of membership in the direct purchaser class, which plaintiffs contend may be determined using Lenovo’s own sales records. Lenovo does, however, argue that plaintiffs have not proposed a feasible method for identifying indirect purchasers.

“Under the law of this circuit, it is enough that the class definition describes ‘a set of

⁵ Plaintiffs also submit expert evidence that that updated version did not completely remove the security vulnerability. *See* Levine Decl, Ex. 44 ¶ 66.

common characteristics sufficient to allow’ an individual to determine whether she is a class member with a potential right to recover.” *Krueger v. Wyeth, Inc.*, 310 F.R.D. 468, 475 (S.D. Cal. 2015) (quoting *In re ConAgra Foods, Inc.*, 302 F.R.D. 537, 566 (C.D. Cal. 2014)). Plaintiffs contend that indirect purchasers may be identified through Lenovo’s records to the extent that consumers registered their purchases with Lenovo or had their computers repaired by Lenovo. Plaintiffs further contend that, to the extent Lenovo’s registration and repair records are inadequate, class members will be able to self-identify by matching their laptop serial numbers against Lenovo’s records to determine whether VisualDiscovery was installed.

Lenovo makes no meaningful challenge to these methods of identifying indirect purchasers. Lenovo does not, for example, explain why its own software installation records could not be used to determine whether putative class members had purchased a laptop with VisualDiscovery installed. The court, therefore, is satisfied that the proposed classes are ascertainable. *See Bias*, 312 F.R.D. at 538 (“Even if a file-by-file review were required to identify borrowers,” class would still be ascertainable where defendant’s records “unquestionably contain information” identifying payments of the charges at issue.).

C. Rule 23(b)(3) Requirements

If the prerequisites of Rule 23(a) are satisfied, the court must then determine whether the class may be certified pursuant to one of Rule 23(b)’s three subsections. In this case, plaintiffs seek certification pursuant to Rule 23(b)(3), which allows class certification if the “court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3).

1. Predominance

The predominance inquiry “tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.” *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 623 (1997). This inquiry requires weighing the common questions in the case against the individualized questions, which differs from the Rule 23(a)(2) inquiry as to whether the plaintiff

can show the existence of a common question of law or fact. *See Dukes*, 564 U.S. at 359. There is “‘clear justification for handling the dispute on a representative rather than an individual basis’ if ‘common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication.’” *Mazza*, 666 F.3d at 589 (quoting *Hanlon*, 150 F.3d at 1022). The predominance inquiry begins with the elements of the underlying causes of action. *See Erica P. John Fund, Inc. v. Halliburton Co.*, 563 U.S. 804, 809 (2011). Plaintiffs’ remaining claims in this action fall into two broad categories: statutory unauthorized access claims (CFAA, California’s Computer Crime Law, CIPA, and trespass to chattels claims) and California consumer protection claims (UCL, CLRA).

a. Unauthorized Access Claims

Plaintiffs’ statutory unauthorized access claims require a showing that Superfish accessed plaintiffs’ laptops and information without permission and that Lenovo conspired with Superfish to make the unauthorized access possible. Plaintiffs’ trespass to chattels claims require a showing that Lenovo intentionally interfered with plaintiffs’ possession of their laptops and that harm resulted. Lenovo does not dispute that its agreement with Superfish and its decision to install VisualDiscovery are subject to common proof. Lenovo argues, however, that individual inquiries are required because of (1) the variations in VisualDiscovery over time, (2) the question of consent, (3) the variations in class members’ use and the many possible explanations for any performance effects they experienced, and (4) the lack of viable class-wide damages model. The court finds that, based on the evidence cited to the court, questions regarding how VisualDiscovery worked and whether class members’ consented can be resolved on a class-wide basis. The court finds, however, that the individualized questions as to whether unauthorized access actually occurred and caused harm outweigh the common questions.

i. Common Questions

The court is not convinced that the changes made to VisualDiscovery over time create questions that cannot be answered on a class-wide basis. Lenovo points to its decisions to shut off HTTPS functionality at the Superfish server in September 2014, to install an updated version of

VisualDiscovery on laptops beginning in November 2014, and to shutoff all functionality at the Superfish server in January 2015. Plaintiffs present expert evidence that the performance and privacy problems remained the same throughout. *See e.g.*, Levine Decl., Ex. 44 ¶¶ 33-36. Moreover, even if changes to the software do affect plaintiffs' claims, such questions do not require an individualized inquiry. The class may need to be limited in the future depending on what the evidence reveals, but the question of how the software operates is subject to common proof.

The question of consent also appears suitable for class-wide resolution. Lenovo argues that consent will have to be determined on a case-by-case basis because some users expressly consented to the operation of VisualDiscovery after being presented with the opt-out pop-up, which provided links to Superfish's Privacy Policy and EULA. "[E]xpress consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the interceptions." *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *15 (N.D. Cal. Mar. 18, 2014). The question of whether the terms of the opt-out pop-up provided adequate notice does not require an individualized inquiry.

Lenovo also argues that the possibility of implied consent presents individualized questions. "Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted." *Id.* at *16. In *In re Google Gmail*, "substantial individual questions regarding the nature of each" defendant's disclosures and the sources to which class members had been exposed predominated on the issue consent. *Id.* at *17-18. Although it is possible that an implied consent defense "could potentially raise individual issues," here, as in *Campbell*, there is a "dearth of evidence" as to any other sources of actual notice that individual class members might have received. *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266 (N.D. Cal. 2016). Plaintiffs claim that Lenovo actively tried to hide VisualDiscovery, and Lenovo cites no evidence to the contrary. Therefore, the court has no basis

for finding that an individualized inquiry is required.

ii. Individualized Questions

Plaintiffs argue that class members' individual experience are not relevant to liability, but Lenovo points to several individualized questions that will predominate in determining liability and damages causation for plaintiffs' unauthorized access claims.

First, all of plaintiffs' unauthorized access claims require a showing that Superfish in fact accessed their laptops and data, and plaintiffs' evidence of unauthorized access is how the VisualDiscovery software works. Yet Lenovo cites evidence that approximately 10% of users uninstalled the software immediately.⁶ *See* Stephenson Decl., Exs. 20, 21. Lenovo also points out that some class members may not have used their laptops for internet browsing and that some may have operated their laptops only on secured networks. Plaintiffs have not explained how their unauthorized access claims could be resolved without conducting an individualized inquiry into these circumstances.

Moreover, "individual causation and injury issues," including whether proposed class member suffered harm as the result of an alleged defect, can make class-wide adjudication "inappropriate." *Wolin, LLC*, 617 F.3d at 1174 (remanding to district court for consideration of whether class could be certified where warranty provided for repair or replacement only if tire wear was "caused by a defect" and noting that tires "deteriorate at different rates depending on where and how they are driven"). Plaintiffs must show that the alleged trespass to chattels "proximately caused injury." *Thrifty-Tel*, 46 Cal. App. 4th at 1566; *see also Sweeney*, 875 N.Y.S.2d at *4. And in order to recover damages or restitution for the alleged CFAA⁷ and Computer Crime Law violations, plaintiffs must show that harm that was attributable to

⁶ Although plaintiffs maintain that VisualDiscovery continued to operate on the laptops after users "opted-out," plaintiffs do not claim that it continued to operate after users uninstalled the software.

⁷ The court also notes that, as discussed in connection with Lenovo's motion to dismiss, there is a statutory minimum loss of \$5,000 under the CFAA. Plaintiffs do not dispute that "absent class members' claims from disparate instances of 'access,'" cannot be aggregated to meet the statutory minimum. *See Halperin v. Int'l Web Servs., LLC*, 70 F. Supp. 3d 893, 900 (N.D. Ill. 2014). Yet plaintiffs do not even attempt to show how minimum losses could be established on any class-wide basis.

defendant's conduct. *See* 18 U.S.C. § 1030(g); Cal. Penal Code § 502(e)(1).

Plaintiffs only evidence of causation is how the software works. *See* Dkt. No. 131 at 20 (citing evidence of Lenovo's own testing). Plaintiffs' damages expert proposes calculations for the market rates for the types of the performance class members would have experienced in the absence of VisualDiscovery. *See* Levine Decl., Ex. 45 ¶¶ 81-102. Plaintiffs propose calculations of how much class members would pay, for instance, for a higher performance CPU, additional gigabytes of RAM, or an incremental increase in internet connection bandwidth. But plaintiffs' expert assumes that amount of harm—the level of decreased performance or the number of gigabytes of RAM used—"could be determined based on analyses by technical experts." *Id.* ¶ 101. Plaintiffs do not explain how a technical expert could determine the amount of damage caused by VisualDiscovery without conducting an individualized inquiry into user-controlled factors affecting performance—such as which ISP class members chose to use, whether class members generally kept their laptops plugged in, and which other programs class members installed on their laptops. *See, e.g.,* Stephenson Decl., Ex. 39 at 171; Ex. 45 ¶¶ 40-43. Therefore, plaintiffs' class-wide damages model "does not even attempt" to "measure only those damages attributable" to the alleged instances of unauthorized access. *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1433 (2013). "[D]amage calculations alone cannot defeat certification." *Pulaski & Middleman, LLC v. Google, Inc.*, 802 F.3d 979, 986 (9th Cir. 2015), *cert. denied*, 136 S. Ct. 2410 (2016) (quoting *Yokoyama v. Midland Nat. Life Ins. Co.*, 594 F.3d 1087, 1094 (9th Cir. 2010)). But "plaintiffs must be able to show that their damages stemmed from the defendant's actions that created the legal liability." *Id.* at 987-88 (citing *Leyva v. Medline Indus. Inc.*, 716 F.3d 510, 513 (9th Cir. 2013) (interpreting *Comcast*, 133 S. Ct. 1426)).

For plaintiffs' CIPA claim, "no separate showing of injury aside from a violation of the privacy rights protected by CIPA is required." *Ades v. Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d 999, 1018 (C.D. Cal. 2014). Instead, any plaintiff "who has been injured by a violation" of CIPA may recover statutory damages from "the person who committed the violation." Cal. Penal Code § 637.2. Plaintiffs' class-wide evidence, however, does not identify any particular "violations" or

1 instances of unauthorized interception; rather, plaintiffs assume, based on the way the software
2 works, that violations occurred on all laptops with VisualDiscovery installed. Plaintiffs do not cite
3 evidence that could be used to determine whether class members actually experienced a statutory
4 violation, and if so, how many. Therefore, plaintiffs cannot show that the statutory damages they
5 seek are attributable to plaintiffs' theory of liability.

6 The cases cited by plaintiffs do not establish that a class may be certified without some
7 way of identifying the statutory violations at issue. The proposed class in *Holloway v. Full*
8 *Spectrum Lending*, No. CV 06-5975 DOC RNBX, 2007 WL 7698843 (C.D. Cal. June 26, 2007),
9 consisted of individuals "who received the same written solicitation." 2007 WL 7698843, at *2.
10 The court found "[a]ny consideration of post-solicitation contact between FSL and individual class
11 members" irrelevant to determining whether a violation occurred and that amount for statutory
12 damages, which ranged "from \$100 to \$1,000 per violations," need not be determined on an
13 individual basis, but rather could be determined based on defendant's conduct in the aggregate. *Id.*
14 at *5. The statutory violations themselves were subject to common proof. Similarly in *Guido v.*
15 *L'Oreal, USA, Inc.*, No. CV 11-1067 CAS JCX, 2013 WL 3353857 (C.D. Cal. July 1, 2013), the
16 court found that "no individualized damages inquiries" were necessary for plaintiffs' GBL claims
17 because a fixed amount would be granted to each class member who purchased the product at
18 issue. 2013 WL 3353857, at *16. Here, plaintiffs' theory of liability is not tied to each purchase of
19 a laptop—as in a false advertising case—but rather to defendants' allegedly unauthorized access.
20 It is not clear, therefore, that each class member would be entitled to any fixed amount. Some
21 purchasers may have experienced no violations at all, while other may have experienced many
22 more than one. In *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 953 (7th Cir. 2006), the Seventh
23 Circuit merely stated that a "representative plaintiff must be allowed to forego claims for
24 compensatory damages" in favor of statutory damages "in order to achieve class certification."
25 The problem here is not that plaintiffs seek statutory damages. The problem is that plaintiffs have
26 not shown how the statutory damages attributable to defendant's unauthorized conduct could be
27 determined.

b. Consumer Protection Claims

With respect to plaintiffs' consumer protection claims, however, the court finds that common questions predominate over any questions affecting individual class members. To establish a UCL claim "based on false advertising or promotional practices, it is necessary only to show that members of the public are likely to be deceived." *Pulaski*, 802 F.3d at 985 (quoting *In re Tobacco II Cases*, 46 Cal. 4th 298, 312 (2009)). A "representative plaintiff need not prove that members of the public were actually deceived by the practice, relied on the practice, or suffered damages." *Ehret v. Uber Techs., Inc.*, 148 F. Supp. 3d 884, 895 (N.D. Cal. 2015) (quoting *Davis-Miller v. Auto. Club of S. Cal.*, 201 Cal. App. 4th 106, 121 (2011), *as modified* (Nov. 22, 2011)). Plaintiffs' CLRA "requires 'an additional showing of reliance.'" *Ehret*, 148 F. Supp. 3d at 901 (quoting *Davis-Miller*, 201 Cal. App. 4th at 125). Reliance, however "can be established on a class-wide basis by materiality." *Id.* (citing *In re Vioxx Class Cases*, 180 Cal. App. 4th 116, 129, 103 Cal. Rptr. 3d 83, 95 (2009) ("If the trial court finds that material misrepresentations have been made to the entire class, an inference of reliance arises as to the class.")). Plaintiffs' UCL and CLRA claims, therefore, are subject to common proof.

Class members' individual experiences with the software are not relevant to whether the laptops were sold with VisualDiscovery installed *See, e.g., Wolin*, 617 F.3d at 1173 ("Although individual factors may affect premature tire wear, they do not affect whether the vehicles were sold with an alignment defect."). As explained in connection with plaintiffs' unauthorized access claims, the changes to VisualDiscovery that Lenovo made over time do not defeat class certification because plaintiffs contend that the all versions had the same performance and privacy effects. Moreover, if the evidence reveals that such changes affect the merits of plaintiffs' fraudulent omissions claims, the merits of plaintiffs' claims could likely still be resolved on a class-wide basis, at least for some subclass of all purchasers.

Lenovo also argues its changing knowledge over time defeats class certification because Lenovo had no duty to disclose anything that it did not know. Specifically, Lenovo argues that it did not know that VisualDiscovery might affect upload and download speeds until Lenovo

received a report from a customer on December 25, 2014.⁸ Plaintiffs claim that Lenovo's own testing showed that effects on upload and download speeds, but it is not clear when the Lenovo conducted the testing. *See* Dkt. No. 131 at 20. In any case, Lenovo's knowledge does not present individual questions as to each class member. Even if the evidence requires an adjustment to the class definitions in the future, the court is satisfied that the question of Lenovo's knowledge is a common one.

Lenovo also argues that plaintiffs' damages model must be rejected as arbitrary, speculative, and unrigorous. As previously noted, "damage calculations alone cannot defeat certification," but "plaintiffs must be able to show that their damages stemmed from the defendant's actions that created the legal liability." *Pulaski*, 802 F.3d at 986-88. Plaintiffs offer two damages models, both of which purport to measure the amount that class members overpaid for their laptops as a result of Lenovo's fraudulent omissions. The first attempts to measure the difference between the actual price paid and the market value of the Lenovo laptops assuming full disclosure of the installation of VisualDiscovery by weighing the negative and positive values of the laptops. The second model calculates the amount of overpayment by attempting out how much of a discount Lenovo would have had to offer in order to persuade consumers to purchase a laptop that came with each of the alleged defects—performance, privacy and security issues—broken down by category.

Lenovo objects that plaintiffs' first model is flawed because, for example, the model assume an average value across laptop models, use a straight-line model for depreciation, and assign no value whatsoever to a laptop with VisualDiscovery installed. Under California law, however, the calculation of restitution damages "requires only that some reasonable basis of computation of damages be used, and the damages may be computed even if the result reached is an approximation." *Pulaski*, 802 F.3d at 989 (quoting *Marsu, B.V. v. Walt Disney Co.*, 185 F.3d

⁸ Lenovo argues that Lenovo did not know about the weak password for the certificate authority in the original version of VisualDiscovery until it was publicly revealed on February 19, 2015, but the court has found that plaintiffs lack standing to pursue claims based on the SSL hijacker security vulnerability.

932, 938-39 (9th Cir. 1999)). Lenovo also objects that the models ignore the benefits of free removal provided by Lenovo, but the “calculation need not account for benefits received after purchase because the focus is on the value of the service at the time of purchase.” *Id.* Plaintiffs’ model may be flawed, but Lenovo has not established that the model is not tied to plaintiffs’ theory of liability.

Lenovo objects to plaintiffs’ second model because it relies on conjoint surveys to determine how consumers would value the laptops’ attributes. *See, e.g.,* Levine Decl., Ex. 45 ¶ 83, Ex. 46. In the cases cited by Lenovo, conjoint analyses were rejected because they looked “only ‘to the demand side of the market equation,’ converting what is properly ‘an objective evaluation of relative fair market values into a seemingly subjective inquiry of what an average consumer wants.’” *In re NJOY, Inc. Consumer Class Action Litig.*, 120 F. Supp. 3d 1050, 1119 (C.D. Cal. 2015) (quoting *Saavedra v. Eli Lilly & Co.*, No. 2:12-CV-9366-SVW, 2014 WL 7338930, at *5 (C.D. Cal. Dec. 18, 2014)) (alteration omitted). In *Saavedra*, the court also noted that in “an ordinary market, price is a proxy for value,” but that “numerous complicating factors in the prescription drug market sever the relationship between price and value,” which rendered the survey results arbitrary. 2014 WL 7338930, at *5. Therefore, these courts found, the damages models could not measure the market value of the products absent the alleged misrepresentations.

The conjoint models proposed by plaintiffs do not suffer from these defects. Plaintiffs’ survey expert “consulted pricing of the Lenovo models at issue, as well as comparable PC laptops” to ensure that the results would “reflect the market,” and addressed “the supply side” of the market, determining that it was not at issue “because all sales of the laptop models at issue have occurred in the past.” Levine Decl., Ex. 46 ¶¶ 17, 46. Lenovo does not identify any complicating factors specific to the laptop market that would render the survey results arbitrary. “[D]isputes about the precision of the particular model [] do not indicate that damages will not be measurable on a classwide basis.” *In re ConAgra Foods, Inc.*, 90 F. Supp. 3d 919, 1030 (C.D. Cal. 2015) (quoting *Khoday v. Symantec Corp.*, No. CIV. 11-180 JRT/TNL, 2014 WL 1281600, at *33 (D. Minn. Mar. 13, 2014)). Therefore, Lenovo’s challenge to class certification based on

plaintiffs' damages models is unavailing.

2. Superiority

Under Rule 23(b)(3), there are four factors pertinent to whether a class action is superior to other available methods for fairly and efficiently adjudicating the controversy:

(A) the class members' interests in individually controlling the prosecution or defense of separate actions;

(B) the extent and nature of any litigation concerning the controversy already begun by or against class members;

(C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and

(D) the likely difficulties in managing a class action.

Fed. R. Civ. P. 23(b)(3)(A)-(D). Plaintiffs argue that a class action is the only realistic method for adjudicating plaintiffs' claims because the potential for recovery for each individual class member is too small, and that no other factors weigh against a finding of superiority.

Lenovo argues that class treatment is not superior because Lenovo has already provided free remedies to class members. Plaintiffs, however, claim that despite the security fixes offered by Lenovo, they have not been compensated for their overpayment. Therefore, a controversy remains.

Lenovo also argues that class certification is not appropriate for the putative nationwide class of indirect purchasers because differences in state law will create difficulties in managing the action. The parties, however, stipulated that plaintiffs will proceed with claims that arise under federal, New York, or California law only until otherwise ordered by the court. Plaintiffs' claims arising under the laws of other states are tolled during the pendency of this litigation or until a court order directs otherwise. Plaintiffs argue that California law should apply to the claims of the nationwide indirect purchaser class because indirect purchasers are intended third-party beneficiaries of the Lenovo-Superfish Business Partnership Agreement, which includes a California choice-of-law provision. Lenovo does not reference the BPA or its choice-of-law provision in its opposition brief. It appears that the choice-of-law question may be resolved on a class-wide basis. Therefore, differences in state law do not create a management obstacle for the

class of indirect purchasers at this time.

D. Conclusion

The parties agree that New York law applies to the direct purchaser class. However, plaintiffs have not demonstrated that class certification is appropriate for any of their claims under New York or federal law. Therefore, the court denies plaintiffs' motion for certification of the direct purchaser class.

The parties agree that California law applies to the California class, and plaintiffs have demonstrated that class certification is appropriate for their California consumer protection claims. Therefore, the court grants plaintiffs' motion for certification of the California class.

The parties have agreed to proceed on the basis of California law, but do not agree that California law applies to the claims of the nationwide class of indirect purchasers. Plaintiffs have demonstrated that class certification is appropriate for their California consumer protection claims. Therefore, the court grants plaintiffs' motion for certification of the indirect purchaser class without prejudice to a motion to decertify on the basis that California law does not apply class-wide.

V. ORDER

Lenovo's motion to dismiss is granted in part and denied in part as follows:

- motion to dismiss plaintiffs' claims for lack of standing is denied;
- motion to dismiss Count I, plaintiffs' Computer Fraud and Abuse Act claim, is denied;
- motion to dismiss Count II, plaintiffs' Electronic Communications Privacy Act claim, is granted;
- motion to dismiss Count IV, plaintiffs' California Unfair Competition Law claim, is denied;
- motion to dismiss Count V, plaintiffs' California Consumer Legal Remedies Act claim, is denied;
- motion to dismiss Count VI, plaintiffs' California Computer Crime Law claim, is denied;
- motion to dismiss Count VII, plaintiffs' California Computer Spyware Act Legal Remedies Act claim, is granted;
- motion to dismiss, Count VIII, plaintiffs' California Invasion of Privacy Act claim, is denied;
- motion to dismiss Count IX, plaintiffs' California negligence claim, is granted;
- motion to dismiss Count X, plaintiffs' California trespass to chattels claim, is denied;

- motion to dismiss Count XI, plaintiffs' New York Deceptive Acts & Practices Statute claim, is granted;
- motion to dismiss Count XII, plaintiffs' New York negligence claim, is granted;
- motion to dismiss Count XIII, plaintiffs' New York trespass to chattels claim, is denied; and
- motion to dismiss plaintiffs' claim for injunctive relief is granted.

Plaintiffs' request for leave to amend is granted. Plaintiffs must file any amended complaint with thirty days of this order.

The court certifies the following classes:

Indirect Purchaser Class (represented by Jessica Bennett, Rhonda Estrella and John Whittle): All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in the United States from someone other than Lenovo.

California Class (represented by Jessica Bennett and Rhonda Estrella): All persons who purchased one or more Lenovo computer models, on which VisualDiscovery was installed, in California.

Pritzker Levine LLP, Girard Gibbs LLP, and Cotchett, Pitre & McCarthy, LLP are appointed as class counsel. Plaintiffs' motion to certify the direct purchaser class is denied.

IT IS SO ORDERED.

Dated: October 27, 2016

Ronald M. Whyte
United States District Judge